UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/727,409	12/04/2003	Richard C. Johnson	ORCL5881	7705

53156 7590 06/24/2008

YOUNG LAW FIRM, P.C.
4370 ALPINE RD.
STE. 106
PORTOLA VALLEY, CA 94028

EXAMINER	
AGWUMEZIE, CHARLES C	
ART UNIT	PAPER NUMBER
3685	

MAIL DATE	DELIVERY MODE
06/24/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/727,409	JOHNSON, RICHARD C.	
	Examiner	Art Unit	
	CHARLES C. AGWUMEZIE	3685	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 October 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *9-13,15-19 and 29-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9-13, 15-19and 29-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

12/4/03; 12/17/03; 8/15/05; 5/9/07

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on October 11, 2007 has been entered.

Acknowledgment

2. Applicant's amendment filed on October 11, 2007 is acknowledged. Accordingly claims 9-13, 15-19 and 29-33, remain pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 29-33**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Brown et al U.S. Patent Application Publication No. 2004/0139327 A1 in view of Hwangbo U.S. Patent Application Publication No. 2003/0154376 A1 and further in view of Sudia et al U.S. Patent Application Publication No. 2005/0204129 A1.

5. As per **claim 29**, Brown et al discloses in a computing environment having a connection to a network, computer readable code readable by a computer system in said environment, for enabling a server computer within the computing environment to both authenticate a user of a client computer within the computing environment and to verify that the user is authorized to request that the server computer carry out a requested action, comprising:

a digital certificate assigned to the user of the client computer, the digital certificate comprising a first code portion and a second code portion, wherein the first code portion of the digital certificate is configured enable authentication of the user, the first code portion defines a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and an extension field;

wherein the second code portion of the digital certificate is configured to define an authority of the user of the client computer to request that the server computer carry out the requested action, the second code portion being configured for inclusion within the extension field of the first code portion, the authority of the user defined within the second code portion of the certificate defining access rights of the user to data and programs within the computing environment (see figs. 1 and 3; 0165; 0067; 0174; 0183), and

code for causing the server computer to carry out steps of:

accessing a store of authority information that is coupled to the network and that is independent of the received certificate (0165, which discloses that the certificate

contains the name of the subscriber, the subscriber's public key, the digital signature of the issuing CA …. And other pertinent information about the subscriber and his organization, such as his authority to conduct certain transactions ….the certificates are stored in an online, publicly accessible repository and are accessed using a standard protocol);

retrieving from the accessed store of authority information stored authority information that is associated with the user (0088, which discloses that the signer may provide a pass phrase or the like to the role identifier 104, after which the pass phrase is compared against a database of pass phrases for various signing roles…);

comparing the retrieved authority information with the authority information included within the received certificate to determine whether the retrieved authority information matches the authority information included within the received certificate (0088, which discloses that if a match is found, the signer is authorized for the corresponding role; 0089, which discloses when a match is found, the corresponding private key is retrieved from the database);

validating the authority information within the received certificate only if the retrieved authority information matches the authority information included within the received certificate (0088 which discloses that if a match is found, the signer is authorized for the corresponding role), and

carrying out the requested action only when the the authority information within the received certificate is successfully validated (0169, which discloses that the certificate includes at least the signer's name and public key…after the certificate is

decrypted, the method continues by determining whether the signer's identity … matches the signer's name in the decrypted certificate, if not the signature verification service 710 terminates with the signature not being verified…see claim 49, which discloses completing the electronic payment request when the payment amount does not exceed the signer's maximum authority; se also fig. 1, 2, 3, and 8; 0165; 0174; 0183; claim 80).

6. What Brown does not explicitly teach is:

the accessed certificate is independent of the received certificate. (However Brown teaches that the information from the decrypted certificate is match against information stored in the database)

a digital certificate assigned to the user of the client computer, the digital certificate comprising a first code portion and a second code portion, wherein the first code portion of the digital certificate is configured enable authentication of the user, the first code portion defines a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and the extension field (Extension fields are inherent in X.509 certificates)

7. Hwangbo discloses a digital certificate assigned to the user of the client computer, the digital certificate comprising a first code portion and a second code portion, wherein the first code portion of the digital certificate is configured enable authentication of the user, the first code portion defines a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and the extension field (fig. 10; 0029; 0034; 0096; claim 17).

8. Sudia et al discloses accessing, over the network, a store of authority information that is independent of the received digital certificate (0132; …authorizing agents who will be empowered to instruct the signing device to apply its partial signature…; 0171; …indicating powers for which the agent is authorized…; 0252; …verifies that the requesting user's signatures matches…)

9. Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the system of Brown et al and incorporate a digital certificate assigned to the user of the client computer, the digital certificate comprising a first code portion and a second code portion, wherein the first code portion of the digital certificate is configured to enable authentication of the user, the first code portion defines a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and an extension field and matching the authority of a user within the second code portion of the certificate to corresponding authority information of the user retrieved from the accessed independent store of authority information in view of the teachings of Hwangbo and Sudia et al respectively since the claimed invention is merely a combination of old and known elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

10. As per **claim 30**, Brown further discloses the computer readable code, wherein the digital certificate conforms to the X.509 standard (0109; 0164; 0183)

11. As per **claim 31** Brown further discloses the computer readable code wherein the second code portion is configured as XML code (0062; 0068; 0069).

12. As per **claim 32**. Brown further discloses the computer readable code, wherein the XML code is compliant with a DSML standard (0062; 0068; 0069).

13. As per **claim 33**. Brown further discloses the computer readable code, wherein the authority of the user of the client computer is stored in a hierarchical authority data structure that is accessible by the server computer (0165 which discloses that the certificates are stored in an online, publicly accessible repository and are accessed using a standard protocol).

14. **Claims 9-13, and 15-19,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Brown et al U.S. Patent Application Publication No. 2004/0139327 A1 in view of in view of Sudia et al U.S. Patent Application Publication No. 2005/0204129 A1.

15. As per **claim 9**, Brown et al discloses a computer-implemented method for ensuring non-repudiation of a payment request, the payment request being generated in a computing environment having a connection to a network, the method comprising the steps of:

receiving, over the network, the payment request together with a certificate identifying a user having caused the payment request to be generated, the certificate including certificate-identifying information and user-identifying information, the certificate further including authority information defining an authority of the user to make the payment request (fig. 1, 2, 3, and 8; 0165; 0174; 0183; claim 80);

validating the certificate-identifying information and the user-identifying information included within the received certificate by accessing a store of authority information that is independent of the received certificate (figs. 1, 2, 3, and 8; 0165; 0067; 0174; 0183; claim 80);

accessing a store of authority information that is coupled to the network and that is independent of the received certificate (0165, which discloses that the certificate contains the name of the subscriber, the subscriber's public key, the digital signature of the issuing CA …. And other pertinent information about the subscriber and his organization, such as his authority to conduct certain transactions ….the certificates are stored in an online, publicly accessible repository and are accessed using a standard protocol);

retrieving from the accessed store of authority information stored authority information that is associated with the user (0088, which discloses that the signer may provide a pass phrase or the like to the role identifier 104, after which the pass phrase is compared against a database of pass phrases for various signing roles…);

comparing the retrieved authority information with the authority information included within the received certificate to determine whether the retrieved authority

information matches the authority information included within the received certificate (0088, which discloses that if a match is found, the signer is authorized for the corresponding role; 0089, which discloses when a match is found, the corresponding private key is retrieved from the database);

validating the authority information within the received certificate only if the retrieved authority information matches the authority information included within the received certificate (0088 which discloses that if a match is found, the signer is authorized for the corresponding role), and

executing of the payment request only when the certificate-identifying information, the user-identifying information and the authority information within the received certificate is successfully validated (0169, which discloses that the certificate includes at least the signer's name and public key…after the certificate is decrypted, the method continues by determining whether the signer's identity … matches the signer's name in the decrypted certificate, if not the signature verification service 710 terminates with the signature not being verified…see claim 49, which discloses completing the electronic payment request when the payment amount does not exceed the signer's maximum authority; se also fig. 1, 2, 3, and 8; 0165; 0174; 0183; claim 80).

16. What Brown does not explicitly teach is:

the accessed certificate is independent of the received certificate. However Brown teaches that the certificates are stored on online publicly accessible repository and that the information from the decrypted certificate is match against information stored in the database.

17. Sudia et al discloses accessing, over the network, a store of authority information that is independent of the received digital certificate (0132; …authorizing agents who will be empowered to instruct the signing device to apply its partial signature…; 0171; …indicating powers for which the agent is authorized…; 0252; …verifies that the requesting user's signatures matches…)

18. Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the system of Brown et al and incorporate a method wherein the accessed certificate is independent of the received digital certificate in view of the teachings of Sudia et al, since the claimed invention is merely a combination of old and known elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

19. As per **claim 10**, Brown et al further discloses the method, wherein the payment request is for a predetermined amount and wherein the payment request is authorized only when the validating steps are successful and when the authority information for the user stored in the hierarchical authority data structure lists an authorized amount for the user at least equal to the predetermined amount (0177; 0183; 0184; 0185).

20. As per **claim 11 and 16**, Brown et al further discloses the method, wherein the certificate received in the receiving step conforms to the X.509 standard (0109; 0164; 0183).

21. As per **claim 12 and 17**, Brown et al further discloses the method, wherein the authority information is configured as XML code (0062; 0068; 0069).

22. As per **claim 13 and 18**, Brown et al further discloses the method, wherein the XML code is compliant with a DSML standard (0062; 0068; 0069).

23. As per **claim 15**, Brown et al discloses a software application configured to carry out a financial transaction, the application being configured to run on a computer coupled to a network, and comprising, stored on a computer-readable medium:

certificate receiving code which is configured to receive a digital certificate from a user over the network, the certificate including certificate-identifying information and user-identifying information, the certificate further including authority information that defines an authority granted to the user to request that the financial transaction be carried out (fig. 1, 2, 3, and 8; 0165; 0174; 0183; claim 80);

certificate validating code configured to enable validation of the certificate-identifying information and user-identifying information within the received certificate (fig. 1, 2, 3, and 8; 0165; 0174; 0183; claim 80) and

authorization validating code configured to cause the computer to carry out steps of:

accessing a data structure that is coupled to the network and that is independent of the received certificate (0165, which discloses that the certificate contains the name

of the subscriber, the subscriber's public key, the digital signature of the issuing CA …. And other pertinent information about the subscriber and his organization, such as his authority to conduct certain transactions ….the certificates are stored in an online, publicly accessible repository and are accessed using a standard protocol);

retrieving from the accessed data structure stored authority information that is associated with the user (0088, which discloses that the signer may provide a pass phrase or the like to the role identifier 104, after which the pass phrase is compared against a database of pass phrases for various signing roles…);

comparing the retrieved authority information with the authority information included within the received certificate to determine whether the retrieved authority information matches the authority information included within the received certificate (0088, which discloses that if a match is found, the signer is authorized for the corresponding role; 0089, which discloses when a match is found, the corresponding private key is retrieved from the database);

validating the authority information within the received certificate only if the retrieved authority information matches the authority information included within the received certificate (0088 which discloses that if a match is found, the signer is authorized for the corresponding role), and

executing of the financial transaction only when the authority information within the received certificate is successfully validated (0169, which discloses that the certificate includes at least the signer's name and public key…after the certificate is decrypted, the method continues by determining whether the signer's identity …

matches the signer's name in the decrypted certificate, if not the signature verification service 710 terminates with the signature not being verified…see claim 49, which discloses completing the electronic payment request when the payment amount does not exceed the signer's maximum authority; se also fig. 1, 2, 3, and 8; 0165; 0174; 0183; claim 80).

24. What Brown does not explicitly teach is:

The accessed certificate is independent of the received certificate. However Brown teaches that the certificates are stored on online publicly accessible repository and that the information from the decrypted certificate is match against information stored in the database.

25. Sudia et al discloses accessing, over the network, a store of authority information that is independent of the received digital certificate (0132; …authorizing agents who will be empowered to instruct the signing device to apply its partial signature…; 0171; …indicating powers for which the agent is authorized…; 0252; …verifies that the requesting user's signatures matches…)

26. Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the system of Brown et al and incorporate a method wherein the accessed certificate is independent of the received digital certificate in view of the teachings of Sudia et al, since the claimed invention is merely a combination of old and known elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

27. As per **claim 19**, Brown et al further discloses the software application, wherein the authority defined by the authority information within the received certificate also defines rights of the user to access predetermined data and programs within the network (0183; 0184).

Response to Arguments

28. Applicant's arguments filed October 11, 2007 have been fully considered but they are not persuasive.

29. With respect to **claim 9**, Applicant argues that the authority of an authorized agent, in Sudia et al is the authority of the authorizing agent to request that his or her associated trusted device digitally sign the document or message, not to request that a server computer carry out a requested action as claimed.

30. In response, Examiner respectfully submits that the agent device acts as the claimed server because the agent device verifies and determines the authority of the agent before signing the document.

31. Applicant further argues that the list of such authorizing agents is maintained in an internal table whereas the current application maintains the authority of the signer in an external database.

32. In response, Examiner submits that the location of the authority database only amount to re-arrangement of parts which does not distinguish the claimed element from the prior art. What is important is the existence of such database whether internal or

external does not matter for the purposes of patentability. However for further information on prior arts that maintains authority database externally see Whitefield U.S. Patent Application No. 2007/0157021. Whitefield made it clear that the received certificate is different from the stored certificate and the information in the received certificate is matched with the information in stored certificate (see 0051).

33. Applicant further argues that the agent device does not include any information as to the authorizing agent's authority within the meaning of the claims.

34. In response, Examiner respectfully disagrees and submits that Sudia does determine the authority of the signer. Even if that is found not to be so, Brown already determines the authority of the signer as shown in the rejection.

35. Applicant further argues that the authority in question is the authority of the user to make a payment request and not the authority of the agent to instruct a signing device to apply a digital signature.

36. In response, Examiner disagrees with Applicant's characterization. However Brown discloses the authority of the user to make a payment request. It is not necessary that Sudia discloses the same information as well.

37. Applicant further argues that a person of ordinary skill in the art in full possession of Brown-Hwangbo-Sudia combination would not be motivated to combine the arts as claimed. That the identity of the authorizing users in such a combination, would be stored within internal tables of trusted signing device as taught by Sudia.

38. In response, the Examiner notes that KSR forecloses the argument that a specific teaching, suggestion, or motivation is required to support a finding of obviousness. See *KSR*, 127 S. Ct. at 1741, 82 USPQ2d at 1396.

Conclusion

39. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The reference cited to Whitfield U.S. Patent Application Publication No. 2007/0157021 A1 is a document considered relevant to the claimed invention.

40. Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art ad are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that the applicant, in preparing the responses, fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

41. Any inquiry concerning this communication or earlier communications from the examiner should be directed to **Charles C. Agwumezie** whose number is **(571) 272-6838**. The examiner can normally be reached on Monday – Friday 8:00 am – 5:00 pm.

42. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Andrew Fischer** can be reached on **(571) 272 – 6779**.

43. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Charlie C Agwumezie/
Primary Examiner, Art Unit 3621
June 19, 2008